UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,847	10/31/2001	Sanguthevar Rajasekaran	020967-001100US	6387

20350 7590 12/18/2002

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
CAPUTO, LISA M	
ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 12/18/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/003,847	**Applicant(s)** RAJASEKARAN ET AL.	
	Examiner Lisa M Caputo	**Art Unit** 2876	

-- Th MAILING DATE of this communication appears on th cov r sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____ .

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 March 2002* is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☒ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4 .
4) □ Interview Summary (PTO-413) Paper No(s). _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: .

DETAILED ACTION

Oath/Declaration

1. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because:
It does not identify the city and either state or foreign country of residence of each inventor. The residence information may be provided on either on an application data sheet or supplemental oath or declaration.

In addition, the application data sheet submitted has the residence information, but the citizenship is not correct for Rammohan Varadarajan. Please correct these items.

Drawings

2. The drawings are objected to because Figures 1-3 and 5-8 should have reference numbers for each step or object so that the invention is claimed completely. In addition, the specification should be amended to include these reference numbers. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

3. The use of the trademarks Visa (page 2 line 20), MasterCard, American Express and Discover (page 5, lines 6-7) have been noted in this application. They should be capitalized wherever they appear and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 6-8 are rejected under 35 U.S.C. 102(b) as being anticipated by Franklin et al. (U.S. Patent No. 6,000,832, from hereinafter "Franklin").

Franklin teaches an electronic online commerce card with customer generated transaction proxy number for online transactions. Franklin discloses that there are three distinct phases supported by the online commerce system 20: a registration phase, a transaction phase, and a payment-authorization phase. During the registration phase, the customer 22 requests an online commerce card from the issuing bank 26. The issuing bank 26 creates an online commerce card for the customer and assigns a customer account number to the card. Additionally, a customer-related secret, such as a private encryption key unique to the customer, is associated with the online commerce card. This customer-related secret can be generated by the issuing bank or selected by the customer. The customer account number and private key are retained in a customer account data record at the issuing bank 26. The "online commerce card" does not necessarily exist in physical form, but in digital form for use in online transactions. The

N-digit customer account number assigned to the online commerce card includes digits for a prefix number for bank-handling information, digits for a customer identification number, digits for an embedded code number, and a digit for a check sum. The number of digits for each portion of the number vary depending upon the card format and control parameters. The commerce card can be configured, for example, to resemble a credit card, a debit card, a bank card, or other type of financial services card. Specific digit formats compatible with a standard 16-digit credit card number are discussed below with reference to FIGS. 5 and 6. The customer account number and customer-related secret are also stored at the customer computer in a password-secured storage location. The issuing bank supplies a software module used to create an embedded code number for each online commerce transaction on the Internet 34. It is noted, however, that the software module may alternatively be packaged as part of can operating system or other product. In this alternative case, the customer may only need an account number and a private key from the issuing bank. The registration phase is described below in more detail with reference to FIG. 2. During the transaction phase, the customer 22 invokes the software module and enters a weak password to gain access to the secure storage location. If the password is correct, the customer computer retrieves the private key and customer account number from storage. The customer computer generates a code number as a function of the private key, customer-specific data (e.g., card-holder's name, account number, etc.) and transaction-specific data (e.g., transaction amount, merchant ID, goods ID, time, transaction date, etc.). Preferably, the customer computer uses a cryptographic hashing function to create a unique, multi-digit MAC (message authentication code) from the various input parameters. The customer computer embeds the code number (or MAC) in the reserved digits of the customer account number to create a temporary transaction number that is specific to a single transaction. It may also be necessary to produce a "check sum" consistent with a proper credit card number. The customer submits the transaction number, with embedded MAC, to the merchant as a proxy for the customer account number during the transaction. The transaction number resembles a real account number. In the case of a credit card, for example, the transaction number resembles a 16-digit, mod 10, credit card number identically formatted with four spaced sets of 4-digits. To the customer, merchant, and every other participant in the transaction, the transaction number appears to be a valid credit card number. Only the issuing bank 26 needs to differentiate the transaction numbers from other real customer account numbers. The customer 22 uses the proxy transaction number in the transaction with the merchant 24. Since the transaction number is issued in place of the customer number for only a single transaction and with a limited life, a thief that intercepts the transaction number is prevented from using it for illicit gain. The transaction phase is described below in more detail with reference to FIGS. 3-6. During the payment authorization phase, the merchant 24 submits an authorization over the conventional payment network 36 to the issuing bank 26 for approval. The authorization request contains the transaction number and the transaction-specific data. The issuing bank 26 identifies the number as a transaction number, as opposed to a real customer account number. The issuing bank 26 locates the customer's data record using the prefix and customer identification portions of the transaction number. The issuing bank 26 retrieves the customer-related secret (i.e., the customer's private key) and customer-specific data from the account data record. The issuing bank 26 then computes a test code number (i.e., a test MAC) as a function of the private key, the customer-specific data, and the transaction-specific data. The issuing bank uses the same cryptographic hashing function as the customer computers. If the test MAC matches the MAC contained in the transaction number received with the authorization request, the issuing bank accepts the authorization request, swaps the customer account number for the transaction number, and processes the request using the customer account number (see Figures 1-7, col 4 line 53 to col 6 line 12).

FIG. 7 shows the online commerce system 20 during a payment authorization phase. This phase involves the merchant 24 seeking authorization from the issuing bank 26 to honor the customer's transaction number received by the merchant in the commerce transaction with the customer. The information exchanges between the merchant computer 30 and the bank computer 32 during the authorization phase are illustrated as enumerated lines. The merchant computer 30 submits a request for authorization over a payment network 36 to the bank computing center 32 (flow arrow 1 in FIG. 7). The authorization request contains the transaction number and the transaction-specific data, such as the amount, time, date, merchant ID, goods ID, and so forth.

The FIG. 7 illustration is simplified for discussion purposes, as other participants will most likely be involved. For instance, the merchant computer 30 typically submits the request for authorization to its acquiring bank (not shown) by conventional means. The acquiring bank validates the authorization request by verifying that the merchant is a valid merchant and that the credit card number represents a valid number. The acquiring bank then forwards the authorization request to the issuing bank. The routing to the issuing bank via the payment network is handled through conventional techniques. When the bank computer 32 receives the authorization request, it first examines the transaction number to determine whether it is a valid number. A transaction number identifier 80 executing at the bank computer 32 examines all incoming account numbers to segregate proxy transaction numbers from real credit card numbers. On a daily basis, it is likely that the bank computer 32 might handle many account numbers (on the order of tens or hundreds of thousands). Most of the numbers are expected to be real credit card account numbers. Only a small percentage is anticipated to be temporary transaction numbers. The transaction number identifier 80 filters out authorization requests that pertain to transaction numbers from authorization request that pertain to real customer account numbers. In the continuing example, the transaction number identifier 80 recognizes the number submitted by the merchant computer 30 as a transaction number based on the first five-to-seven digit prefix. The transaction number identifier 80 passes the transaction number to the account manager 60. The account manager 60 uses the transaction number as an index to transaction records in the customer database 62. More particularly, the account manager 60 utilizes the prefix and customer ID portions of the transaction number (i.e., the first nine-to-eleven digits) to identify a customer account. If no records are found, the number is deemed invalid and the bank computer 32 returns a message disapproving the transaction to the merchant computer 30. If a record is found, the account manager 60 retrieves the customer's private key and customer-related data from the customer data record. The account manager 60 also extracts the MAC from the transaction number. The account manager 60 submits the private key, the customer-related data, and the transaction-specific data to the MAC coding and comparator unit 82. The MAC coding and comparator unit 82 derives a test MAC from the private key, the customer-related data, and the transaction-specific data using the same function employed at the customer computer. Preferably, the same cryptographic hashing function is used. The MAC coding and comparator unit 82 compares the test MAC with the embedded MAC from the transaction number. If the two MACs match, the bank has a very high degree of certainty that the transaction number is valid and originated from the customer. Once the transaction number is verified, the account manager 60 substitutes the customer account number in place of the transaction number in the merchant authorization request. The account manager 60 then submits the authorization request to the bank's traditional processing system 84 for normal authorization processing (e.g., confirm account status, credit rating, credit line, etc.). After the request is processed, the processing system 84 returns an authorization response to the account manager 60. The account manager fetches the transaction number and substitutes the transaction number in place of the customer account number in the bank's authorization reply. The bank computing center 32 then returns the authorization reply to the merchant computer 30 via the payment network 36 (flow arrow 2 in FIG. 7). In this manner, the merchant always handles the transaction number as if it is a real credit card number (see Figures 1-7, col 11 line 25 to col 12 line 42).

Regarding claims 7-8, Franklin teaches that this customer-related secret (private encryption key) can be generated by the issuing bank or selected by the customer. In addition, during an online commerce transaction phase, a proxy number suitable for a transaction is generated that resembles the customer account number but has a code number embedded in it that is derived at least in part on the customer-related secret. Hence, the customer has input to the challenge (see claim 1 of Franklin reference). Hence, Franklin teaches that a one-time use card is generated, authenticated, transmitted, verified, and used for transactions.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

6. Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al. (U.S. Patent No. 6,000,832, from hereinafter "Franklin") in view of Linehan et al. (U.S. Patent No. 5,495,533, from hereinafter "Linehan"). The teaching of Franklin has been discussed above.

Franklin teaches that a challenge is generated at the client when the commerce card is created at the client, the challenged is signed with the private encryption key, the challenge is sent to the server when the customer submits the transaction number, and the signature is verified when there is an authorization over the payment network. Franklin teaches that the indication of successful authentication is sent to the merchant and not the client. In addition, the customer-related secret can be generated by the issuing bank or selected by the customer (this number generation is sequential as recited in claim 3 of the instant application because the numbers are generated in a sequence and hence are easier to troubleshoot if necessary).

Regarding claim 1, Franklin fails to teach that the successful authentication indication is sent to the client.

Linehan teaches a personal key archive. Linehan teaches that A broad aspect of the present invention is a a computing system having a security system for identifying if a user is permitted to create or access a data file on the computing system. The computing system has an authentication server; a key client; a key generator; a key server; a key database; an encrypted data file memory; the authentication server authenticates the user as permitted accessing the computing system the authentication server provides the user with a ticket validating the user as permitted to operate on the computing system; the key client of a creating user when a creating user creates a data file invokes the generator to generate a key corresponding to the data file; the key is provided to the key server; the key client of the creating user uses the key to encrypt the data file to form an encrypted data file which is stored in the encrypted data file memory; the key client of an accessing user, when an accessing user accesses the data file, sends the ticket and said data file identification data to the key server; the key server checks the ticket to verify that the accessing user is permitted to access the data file; the key server sends the key corresponding to the data file to the key client of the accessing user; and the key client of the accessing user uses the key to decrypt the encrypted data file (see col 4 line 61 to col 5 line 16). Hence, Linehan teaches that the indication is sent to the client when authentication server provides the user with a ticket that validates the user.

In view of the teaching of Linehan, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the electronic commerce system of Franklin with the authenticating computing system of Linehan, and to employ a method to notify the client directly so that the system is time efficient and the message did not get misinterpreted through the merchant server.

Regarding claim 2, Franklin fails to teach that the challenge comprises generating a random number.

Linehan teaches that in the basic method, each data file is encrypted by the Personal Key Client, on the user's computer, using a randomly-chosen key generated by the Personal Key server at the time the file is created (see col 7, lines 15-38).

In view of the teaching of Linehan, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ random key generation because it is a more secure way of generating numbers. It is well known in the art that random numbers are harder to decode because of their nature of not having a specific pattern.

Regarding claims 4-5, Franklin teaches that this customer-related secret (private encryption key) can be generated by the issuing bank or selected by the customer. In addition, during an online commerce transaction phase, a proxy number suitable for a transaction is generated that resembles the customer account number but has a code number embedded in it that is derived at least in part on the customer-related secret. Hence, the customer has input to the challenge (see claim 1 of Franklin reference).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: U.S. Patent No. 6,076,069 to Laor which discloses a method for distributing and redeeming electronic coupons, U.S. Patent No. 6,317,838 to Baize which teaches a method and architecture to provide a secured remote access to private resources, and U.S. Patent No. 5,657,388 to Weiss which discloses a method a apparatus for utilizing a token for resource access.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ***Lisa M. Caputo*** whose telephone number is **(703) 308-8505**. The examiner can normally be reached between the hours of 8:30AM to 5:00PM Monday through Friday. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on 703-305-3503. The fax phone number for this Group is (703)308-7722, (703)308-7724, or (703)308-7382.

Communications via Internet e-mail regarding this application, other than those under 35 U.S.C. 132 or which otherwise require a signature, may be used by the applicant and should be addressed to [**lisa.caputo@uspto.gov**].

All Internet e-mail communications will be made of record in the application file. PTO employees do not engage in Internet communications where there exists a possibility that sensitive information could be identified or exchanged unless the record includes a properly signed express waiver of the confidentiality requirements of 35 U.S.C. 122. This is more clearly set forth in the Interim Internet Usage Policy published in the Official Gazette of the Patent and Trademark on February 25, 1997 at 1195 OG 89.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 308-0956.

LMC
December 13, 2002

MICHAEL G. LEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2800